IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH AND SEIZURE WARRANT FOR A CELLPHONE CURRENTLY IN THE POSSESSION OF THE ATF BALTIMORE FIELD OFFICE IN BALTIMORE, MARYLAND	**Case No.** 1:21-mj-1616 TMD

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Anthony Petrella, Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), being duly sworn, depose and state as follows:

I. PURPOSE OF THIS AFFIDAVIT

1. I submit this affidavit in support of a search warrant authorizing the search of a white Apple iPhone bearing FCCID #BCG-E3085A ("**SUBJECT TELEPHONE**"), further described in Attachment A and in the custody of the ATF Baltimore Field Office in Baltimore, Maryland.

2. I submit that there is probable cause to believe that the **SUBJECT TELEPHONE** contains evidence, fruits, and instrumentalities of the crime of possession of a firearm by a convicted felon, in violation of 18 U.S.C. § 922(g)(1). The search warrant would authorize members of the ATF, or their authorized representatives including other law enforcement agents assisting in the above described investigation, to examine the **SUBJECT DEVICE** for the purpose of seizing electronically stored data described in Attachment B.

3. I submit this affidavit for the limited purpose of establishing probable cause for a search warrant. I have not included every fact known to me concerning this investigation to date.

Rather, I set forth only those facts I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause. The information set forth in this affidavit derives from my personal knowledge and observations; discussions with other law enforcement officers and witnesses; and my review of police reports and public records. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

II. AFFIANT BACKGROUND

4. I am "an investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

5. I have been a Special Agent with ATF since 2020 and am currently assigned to the ATF Baltimore Field Division, Group III. I attended the Department of Homeland Security's Criminal Investigator Training Program and ATF's Special Agent Basic Training for a combined period of 26 weeks. I served as a federal police officer with the Supreme Court of the United States Police Department in Washington D.C for approximately six years before working for ATF.

6. I am currently participating in investigations concerning the illegal possession of firearms, controlled substance laws, and the commission of violent crimes by organized gangs. I received specialized training and personally participated in various types of investigative activities, including, but not limited to: (a) physical surveillance; (b) the debriefing of defendants, witnesses, informants, and other individuals who have knowledge of firearms and controlled substance laws; (c) code words and phrases used by criminals when referencing firearms and narcotics; (c) undercover operations; (d) the execution of search warrants; (e) the consensual monitoring and

recording of conversations; (f) electronic surveillance through the use of pen registers and trap and trace devices; and (g) the handling and maintenance of evidence; and (i) Title III investigations.

III. AFFIANT EXPERTISE

7. Based on my training, knowledge and expertise I know the following about persons engaged in unlawful firearms possession and firearms trafficking and the use of cellphones in furtherance of these activities:

a. The fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital camera technology is often used to capture images of tools and instrumentalities of pending criminal activity, like firearms. The **SUBJECT TELEPHONE** has both digital storage capacity and digital camera capabilities.

b. Criminals often place nominal control and ownership of telephones and other electronic devices in names other that their own to avoid detection of those telephones by government agencies. Even though these are in the names of other people, criminals retain actual ownership, control, and use of the telephone and/or device, exercising dominion and control over them.

c. Criminals often use different types of communication devices and change the numbers to these communication devices frequently. This is done to avoid detection by law enforcement personnel.

d. Cellular phones and other electronic devices capable of sending and/or receiving communications associated with criminals include various types of evidence. Phones may contain relevant text messages or other electronic communications; they may contain electronic address books listing the phone numbers and other contact information associated with co-conspirators; and they may contain other types of information.

e. Criminals who engage in criminal activity with others take photos of themselves with high-end consumer items, like cars or watches and other items they acquired during the crime. These "trophy" photos are often maintained on cellular telephones and electronic devices to be shared on social media, or as symbols of their success.

f. Persons prohibited from possessing firearms will often utilize unlawful means of obtaining them such as burglary, theft, or trading them for narcotics. Information surrounding the unlawful transfer of firearms and their prohibited possession is often memorialized within the possessor's cell phone.

g. Cellular telephones may contain location information that indicate where a user of the cellphone was located before, during and after a crime has occurred.

h. The mere fact of a cellular phone's call number, electronic serial number or other identifying information may be of evidentiary value as it may confirm that a particular cell phone and/or electronic device is the phone identified during a wiretap, pen register, or other electronic investigation.

IV. PROBABLE CAUSE

8. On April 19, 2021, at approximately 1:07 a.m., Maryland Department of Transportation Authority (MDTA) Police Officers were on routine patrol on interstate I-95 south when they were alerted by dispatch of a crashed vehicle in Bore 2 of the Fort McHenry Tunnel. Dispatch advised that the occupants abandoned the crashed vehicle and had begun to walk southbound inside Bore 2. The Authority Operations Center (AOC), having the capability of monitoring cameras inside the tunnel, advised the officers that the occupants of the vehicle could no longer be seen in Bore 2. MDTA officers responded to the area traveling down Bore 1 and observed individuals walking southbound inside the bore along the left-hand side catwalks.

Officers also observed an abandoned brown bag on the ground of the catwalks as the individuals were walking past the area. Officers recovered the bag and placed it in their patrol vehicle while continuing to follow the individuals through the tunnel.

9. Once the five individuals, including an individual later identified as Dantre HILL, arrived at the end of the tunnel, they were detained by MDTA. Officers retrieved the abandoned brown bag from their patrol vehicle and conducted a search. Recovered from the bag was a Bersa, model BP9CC .9mm pistol bearing serial #G95353 loaded with eight rounds of 9mm ammunition and the **SUBJECT TELEPHONE**. All five individuals were read their Miranda rights including HILL. Upon being questions, all five individuals, including HILL, denied ownership of the bag and denied dropping it on the catwalk. The Officers then arrested and transported all five individuals back to the MDTA Central Command Station along with the brown satchel bag and its contents.

10. When officers connected the **SUBJECT TELEPHONE** to a charger, a picture of HILL was visible from the locked home screen. Officers were also able to match HILL's tattoos on his arm to the tattoos visible on the locked home screen.

11. Officers reviewed recorded video footage of the cameras inside the Fort McHenry Tunnel and saw a black male wearing an orange hat and a brown jacket who matched the physical characteristics of HILL flee the crashed vehicle carrying a brown bag. HILL was again read his Miranda rights and transported to Baltimore Central Booking Intake Facility.

12. I have reviewed HILL's criminal record and learned that in 2018 he was convicted of conspiracy to distribute narcotics in the United States District Court for the District of Maryland. HILL was sentenced to two years imprisonment and is currently on federal supervised release. Therefore, HILL is prohibited from possessing firearms and ammunition pursuant to 18 U.S.C.

§ 922(g)(1). Moreover, based on this prior conviction, I believe HILL was aware that he had previously been convicted of a crime punishable by more than one year in prison.

13. I have reviewed the information regarding the Bersa firearm recovered and believe that it is a firearm as it is defined under federal law. I further believe that the firearm was manufactured outside the state of Maryland and therefore, the firearm affected interstate commerce prior to its recovery in Maryland on April 19, 2021.

V. FORENSIC ANALYSIS OF ELECTRONIC COMMUNICATIONS DEVICES

14. Based on my training, I know that electronic devices such as cellular phones (smartphones) can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the **SUBJECT TELEPHONE** may still be stored on those devices, for various reasons, as discussed in the following paragraphs.

15. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT TELEPHONE** was used, the purpose of its use, who used it, and when.

16. There is probable cause to believe that this forensic electronic evidence might be stored within the **SUBJECT TELEPHONE** because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs

store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

17. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

18. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

19. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

20. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion

onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

22. Additionally, the only known specifics the phone requested for authorization to search are detailed in Attachment A and the types of information expected to be recovered from the devices are listed in Attachment B.

VI. CONCLUSION

23. Wherefore, in consideration of the facts presented, I respectfully request that this Court issue a search warrant for the **SUBJECT TELEPHONE** and authorize the search for the information set forth in Attachment B, where applicable, which constitute fruits, evidence and instrumentalities of possession of a firearm by a prohibited person in violation of 18 U.S.C. § 922(g).

24. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice for 30 days from the date that the execution of the warrant is completed. This delay is justified because there is reasonable cause to believe that providing immediate notification of the execution of this warrant may have an adverse result on this investigation, as defined in 18 U.S.C. § 2705. In many cases due to advanced encryption technology and passwords used in modern cellular phones, a significant amount of time may elapse between when law enforcement begins to execute the warrant, and when the device can be searched or the evidence described in Attachment B can be recovered. Providing immediate notice would seriously jeopardize the ongoing investigation, as such a disclosure would give persons an opportunity to destroy evidence (I am aware that applications exist to remotely delete data from cellular devices), change patterns of behavior, notify confederates, which may cause the confederates to change their use of certain cellular

devices or destroy evidence from their accounts identified through the execution of this warrant, and may afford them the opportunity to flee from prosecution.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge.

ANTHONY PETRELLA

Digitally signed by ANTHONY PETRELLA
Date: 2021.05.28 09:06:03 -04'00'

Special Agent Anthony Petrella
Bureau of Alcohol, Tobacco, Firearms and Explosives

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on June 1, 2021.

Hon. Thomas M. DiGiralomo
United States Magistrate Judge

ver: Apr 20

ATTACHMENT A
Device to be Searched

A white and pink Apple iPhone with a silver and black case bearing FCCID #BCG-E3085A (**SUBJECT TELEPHONE)** currently located in the possession of the ATF Baltimore Field Office in Baltimore, Maryland.

ver: Apr 20

ATTACHMENT B
ITEMS TO BE SEIZED

All records contained in the **SUBJECT TELEPHONE** (described in Attachment A), which constitute evidence of violations of 18 U.S.C. §§ 922(g) (prohibited person in possession of a firearm) including the following items, as outlined below:

1. Contact logs that refer or relate to the user of any and all numbers on the **SUBJECT TELEPHONE**.

2. Call logs reflecting date and time of received calls.

3. Any and all digital images and videos of persons associated with this investigation.

4. Text messages to and from the **SUBJECT TELEPHONE** that refer or relate to the crimes under investigation.

5. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation.

6. Voicemails that refer or relate to the crimes under investigation.

7. Voice recordings that refer or relate to the crimes under investigation.

8. Any data reflecting the phone's location.

9. Contact lists.

10. Any and all records related to the location of the user(s) of the devices.

11. Evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries,

configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

12. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

13. evidence of the lack of such malicious software;

14. evidence of the attachment to the **SUBJECT TELEPHONE** of other storage devices or similar containers for electronic evidence;

15. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Devices;

16. evidence of the times the **SUBJECT TELEPHONE** was used;

17. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT TELEPHONE**;

18. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the **SUBJECT TELEPHONE**;

19. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash

drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

2. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

3. "scanning" storage areas to discover and possible recover recently deleted files;

4. "scanning" storage areas for deliberately hidden files; or

5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.